シリアル番号付き暗号化ＱＲシンボルを用いた偽造抑止

株式会社テララコード研究所
寺浦　信之

１．　はじめに

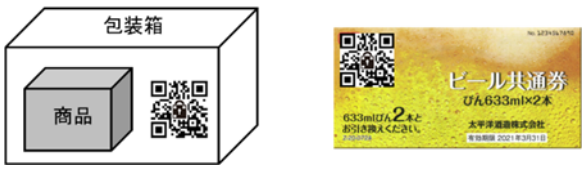
当社では、既存のバーコード（1 次元シンボル）や二次元コード（2 次元シンボル）について、互換性を維持しつつセキュリティ機能を付加する手法を開発し、偽造防止等を目的とした提案を行ってきた。

今回、シリアル番号付き暗号化ＱＲシンボルとその検証システムを開発した。そこで、開発したシンボルと機器、及びそれらを用いた偽造抑止の応用システムを紹介する。また、シリアル番号付き QR シンボルを透明化して、より偽造抑止効果を向上させる手法についても紹介する。

なお、本稿では、JIS[1)]や ISO／IEC[1)]で規定されているシンボルを QR コードと呼び、互換性を有しないが同等の構成、外観を有するシンボルを QR シンボルと呼ぶ。

２．偽造の手段及びその抑止の考え方

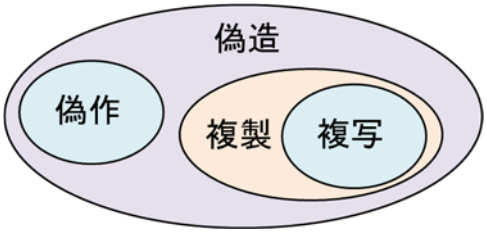
商品や書類（以下、商品等）に、第１図に示すように、例えば物であれば包装に、書類であれば書類そのものにシンボルを付し、シンボルの正当性を判断することにより、商品等の正規性を判断する。そこで、以下の議論での偽造対策及び検証の対象は、商品等に付帯させるシンボル（QR シンボル）である。



第１図　包装または書類へシンボルを付帯

２．１　偽造の手段

シンボルの偽造は、第２図に示すように、偽作、複製、複写によってなされる。ここで、偽作とは、正規品とは独立して正規品と同等のシンボルを生成することである。それに対して、複製は正規品を入手して、シンボルの構成を解析する等によって、当該正規品と同じシンボルを生成することである。また、複写は正規品をコピー機を用いて正規品と同じシンボルを生成することであり、複製の一つの手段である。複写は最も容易な偽造手段である。

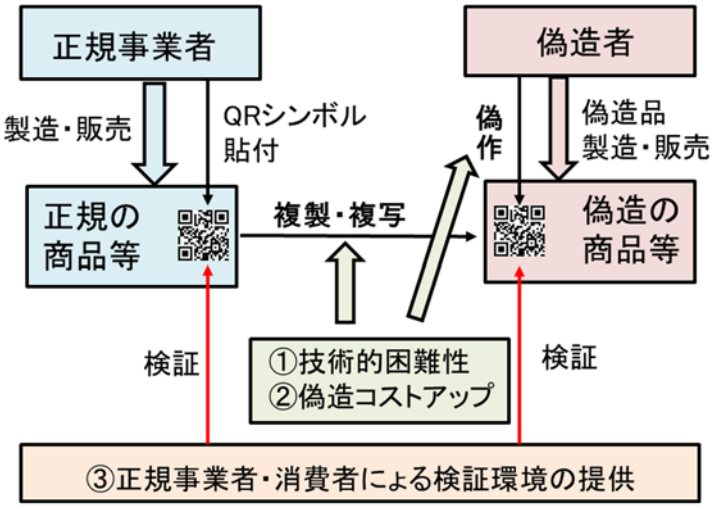


第２図　偽造の手段

２．２　偽造抑止の考え方

シンボルの偽造は、上記の三つの手段によってなされるので、これらを何らかの方法で阻害し、困難化することによって抑止することが可能となる。また、検証手段の存在が不可欠である。そこで、以下の三つの基本的な考え方によって、偽造抑止を実現する。

偽造抑止の戦略を第３図に、またそれを具体的に実現する対応手段を第１表に示す。



第３図　偽造抑止戦略

第１表　偽造抑止の対応策

戦略項目	対応手段	偽作	複製	複写
技術的困難性	暗号化	○		
	透明化			○
	電子署名	○		
コストアップ	シリアル番号		○	○
検出環境整備		○	○	○

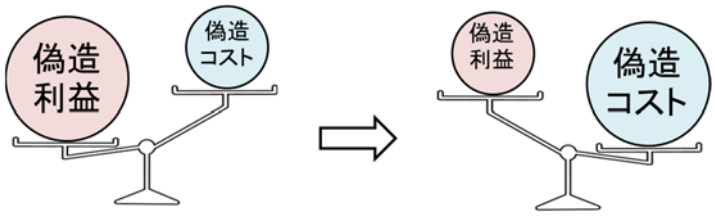
２．２．１　技術的困難化

偽造抑止の第１の考え方は、技術的困難化である。正規品のシンボルと同等のシンボルを作成することが困難な技術的手段を用いて正規品を生成し、偽造の障壁とする。その偽造防止の対応策の例を、三つの偽造の手段への効果と共に第１表に示している。

この中で、暗号化は情報技術を用いた偽作の困難化手法であり、正規品生成のコスト負荷が小さく、優れた手法である。暗号化は、偽造手段の偽作を事実上不可能とするので、不可欠の技術である。今回、開発したシリアル番号付き暗号化ＱＲシンボルでは、独自の暗号化手法を用いている。暗号化手法について、次節で概説する。

２．２．２　偽造コストアップ

偽造抑止の第２の考え方は、偽造コストアップである。偽造者の目的の第１は経済的な利益と考えられるので、偽造のコストを増大させることにより、経済的な利益を低減し、偽造を経済的に成立させず、その動機を失わしめる（第４図）。



第４図　偽造コストアップ

上記に示した偽造の３つの手段の中で、複製を防止することは事実上不可能である。例えば、ＱＲシンボルであれば、例え暗号化されていても、ＱＲシンボルを構成するセルは白と黒のセルから構成されており、このセルを同じ構成で再現すると複製が可能となる。

偽造コストアップの主たる目的は、複製の防止である。　一つを解析し、その複製のシンボルを作成する費用がＡ円とすると、１万個のシンボルを複製するには１万ｘＡ円を要すると期待できる。そこで、正規品のシンボルを全て異なるものとする。

２．２．３　検出環境の整備

偽造抑止の手段を講じても、正規品か偽造品かを判断する検証手段が無ければ、抑止の効果は皆無である。事業者が市場調査によって偽造品の存在を認識し、その排除をする努力が重要である。また、消費者自らが、購入の時点で目前の商品を判定し、偽造品であれば購入しない行動をとれば、偽造品は販売されず、偽造者の利益は低減し、偽造のマインドは低下する。

そこで、事業者及び消費者が検証する手段を提供し、検出環境を整備する。

３．　偽造抑止手段

３．１　技術的困難化

３．１．１　暗号化ＱＲシンボル

ＱＲシンボルを、共通鍵を用いて暗号化する手法としては、収容するデータを暗号化して収容する方式（データレベル暗号化）とシンボルとして暗号化する方式（シンボルレベル暗号化）がある。前者は構造上ＱＲコードそのものであり、暗号化データは誤り訂正を経て一旦読取られる。その後、平文に復号される。そこで、この方式では暗号化データが偽造者に解析される可能性がある。一方、後者はＱＲコードで誤り訂正に用いられているＲＳ符号に着眼し、多くの誤りを与えることで復号をできなくする方式である。収容データの外側の処理であるので、アプリケーションが意識することなく、スキャナ等が復号処理し、データを読取ることが可能である。また、既存の読取り装置等では、そのデータの一部も読取ることはできない。

第２表に暗号化ＱＲシンボルを示す。暗号化ＱＲシンボルは、透明化せずそのままの形態でも真贋判定や秘匿データの受渡しに用いることが可能であるが、透明化することでより大きな効果を発揮すると期待できる。

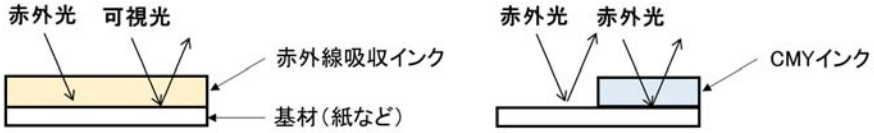
第２表　暗号化 QR シンボル

項目		QRコード	暗号化QRシンボル	
			通常印刷	透明印刷
シンボル画像				
作成と読取り		①誰でも作成可能 ②誰でも読取可能	①当社のみ作成可能 ②当社提供手段のみ可能	
暗号化		無し	独自のシンボルレベルの暗号化	
視覚性		見える	見える	見えない
読取り	光	可視光	可視光	赤外線
	装置	スマホ、スキャナ	スマホ、専用スキャナ	専用スキャナ
偽造抑止性	偽作	×	○（暗号化）	○（暗号化）
	複製	×	△（シリアル番号）	△（シリアル番号）
	複写	×	△（シリアル番号）	○（透明化）

３．１．２　透明化

透明化は、印刷技術を用いた複製、複写の困難化手法である。赤外線吸収インクでシンボルを印刷し、赤外光を用いてシンボルの読取りを行う。可視光では、シンボルは透明であるので、目には見えないので、人はその存在に気がつかない。また、通常の読取り装置では、読取りができない。そして、コピー機では複写することができない[2)]。

透明化は、先に述べたように、赤外線吸収インクを用いて QR シンボルを印刷する。この時、第５図に示すように、可視光については、インクを透過し、印刷する下地の紙で反射されるので、QR シンボルは透明となる。一方、赤外光の場合には、インクで吸収され、赤外光は反射されないので、QR シンボルの黒セルは黒色となり、白セルは紙で反射され白色なり、QR シンボルが浮かび上がり、読取り可能となる。



第５図　赤外線吸収インクと赤外光の特性

３．１．３　電子署名

今回のシステムでは、採用しないが、記憶された情報の改ざんを防止する方法として、電子署名を付す方法がある。電子署名は現在用いられている情報システムのセキュリティを支える基本技術であるＰＫＩの仕組みである。より高い偽造防止システムを構築する場合に用いる方法である。本稿では、通常及び中レベルのセキュリティシステムを対象としているので、詳細については、参考文献[3)]を参照していただきたい。。

参考までに、第６図に電子署名付き QR シンボルを示す。データ部は通常暗号化されず、QR コードと互換性があるので、通常の読取り装置で読取り可能である。暗号化が不要であるのは、内蔵されている電子署名の作成に用いる秘密鍵が秘匿されており、偽造者には知り得ず、偽作が不可能であるからである。

第６図　電子署名付き QR シンボル

３．２　困難化技術の選択

前節で示した困難化技術は、必要とされるセキュリティレベルに応じて、選択され、組合せて併用される。セキュリティレベルと組み合わせ対応を第３表に示す。

ここで、暗号化は必須の技術であり、透明化はより高度なセキュリティレベルで選択される。さらに、改ざんが懸念される高度なレベルが要求される場合には、電子署名が使用される。

以下では、暗号化を必須とし、透明化をオプションとして説明する。透明化をオプションとしたのは、シリアル番号によって透明化の最大の効果である複写防止の効果が見込めるからである。

第３表　対応手段の組合せ

対応手段	セキュリティレベル		
	通常	中度	最大
暗号化	○	○	○
透明化		○	○
電子署名			○
シリアル番号	○	○	○

３．３　シリアル番号の導入

前記の暗号化によって、偽作が防止可能となる。そこで、残る偽造の手段は複製（複写）である。既に述べたように、ＱＲシンボルでは、そのセルの白、黒を特定すれば、複製は可能となる。シンボル画像の宿命である。しかし、複製にはセル色の特定が必要となる。そして、その後ＱＲシンボル画像が再構成される。また、通常印刷では撮像されたシンボル画像が偽造シンボルとして用いられる。

この複製（複写）過程で工数（コスト）が発生する。単一の暗号化ＱＲシンボルを、全ての商品等に用いていれば、複製された画像は、正規の暗号化ＱＲシンボルであり、正規品と判別することはできない。一方、正規品の暗号化ＱＲシンボルが全て異なるデータを収容し、全て異なるシンボル画像となる場合では、状況は異なる。偽造者は１個１個について、異なるシンボル画像を正規品から複製（複写）する必要があるからである。例えば、１０００個の偽造品の画像を作成するためには、１０００個の正規品の画像を上記の手段によって複製（複写）する必要があり、相当の工数を要し、コストアップとなる。同数の正規品を入手する必要がある点は、コストアップの大きな要因となる。

これによって、偽造者の利益は大きく低減し、または利益を得る事ができなくなる等期待する利益を実現できない場合には、偽造を行わないと考えられる。

収容データを全て異なるデータとする為に、シリアル番号を用いる。収容データの構成については、別途説明する。

４．暗号化 QR シンボル画像とデータ構成

４．１　暗号化 QR シンボルの画像

暗号化 QR シンボルの画像として、第４表に示す画像を提供する。第４表に示すように、中央部または右下部にセキュリティ QR マーク（SQR マーク）を付したシンボル画像を提供する。これは、SQR マークが付されていない暗号化 QR シンボルは、一見、QR コードのように見えるが、スマホなどの通常の読取り手段では、読取ることができない。スマホで読もうとした一般ユーザにとっては、不可思議なこととである。そこで、SQR マークを付して、QR コードではなく暗号化 QR シンボルであることを明示する。

SQR マークの表示は、偽造防止手段を講じていることを、消費者だけでなく、偽造を行おうとしている者に対しても示している。通常の読取り装置で読めない QR シンボルとそれに付された SQR マークによって、偽造者に心理的な障壁を設ける。

第４表　提供するシンボル画像

項目	SQRマーク無し	SQRマーク有	
		中央配置	右下配置
シンボル画像			
バージョン	V2、V3	V2、V3	V2、V3
主な対象	透明シンボル用	通常シンボル用	通常シンボル用
特長	・QRコードと同等 ・目立たない	・セキュリティ性明示	・セキュリティ性明確に明示

４．２　データ構成

暗号化 QR シンボルに収容するデータについて説明する。

①データ量

収容するデータの長さは第５表に示すように、用いる QR シンボルのバージョン（論理的サイズ）と SQR マークの有無によって異なる。

偽造抑止用の QR シンボルでは、必要なデータ量は比較的少ないと想定される。そこで、提供する画像のバージョンは、バージョン２（V2）とバージョン３（V3）に限定した。V2 では、SQR マーク無しでは２９英数字であり、有りの場合では、２０英数字である。また、V3 では、それぞれ４７、３５英数字となる。使用するデータ量によって、V2 または V3 を選択する。

SQR マークが有る場合には、データを正しく保持するセルの数が少なくなり、保持可能なデータ量が少なくなる。

第５表　データ量

項目	バージョン（収容データ桁数）	
SQRマーク種別	V2	V3
SQRマーク無し	29	47
SQRマーク中央	20	35
SQRマーク右下	20	35

②データ構成

収容するデータは、第７図に示すように、固定部とシリアル番号部から構成される。固定部は、使用者毎に、または対象毎に割当てられた英数字列であり、使用者が指定することが可能である。シリアル番号部は、システムによって自動的に割り当てられ、その長さは予め使用者が指定する。

第７図　データ構成

③データ構成の例

データ構成の例を、第６表に示す。

例１は、ブランド型である。固定部にはブランドを示す文字列を配置する。この場合では、各企業で同じ固定部を用い、複数の商品や仕向け先の管理は、シリアル番号の割り当てで行う。また、英数字を付加して製品型名とする拡張も可能である。例１は、主に一般ユーザが判定する場合に用いられる。

例２は､JAN コード型である｡固定部には対象となる商品の JAN コードを配置する。この場合には、商品毎にシリアル番号を与えて管理を行う。また、出荷先の企業や国名を付加して、流通調査が可能な拡張も可能である。例２は、主に事業者が調査を行うために用いられる。

例２の拡張として、流通調査用の仕向け国の追記を示したが、仕向け先（会社）など対象を特定し、限定する拡張も可能である。例３は、仕向け先の機器を特定するものであり、当該機器としては、特殊な印刷機や検査装置がある。この場合、シリアル番号付き QR シンボルを貼付する対象は、特殊なインクや試薬である。この機器指定型では、当該機器で機器番号をチェックし、機器番号が一致しなければ複製品と判断する。これ

により、対象となる機器が市場で多く稼働している場合、シリアル番号の使用履歴チェックが不可の場合でも、ローカルシステムで対応可能となる。但し、このような使用法では、先に述べた透明化を行い、複製、複写を不可とすることが望ましい。従って、シリアル番号による防壁は、透明化による防壁が破られた場合の二次防壁と言える。

第６表　データ構成の例

項目		固定部	シリアル部
データ	種別	英数字、記号	数字
	長さ	4～30桁	4～10桁
例	例1：ブランド型	TCODE	0001
	・ブランド型の拡張	TCODE123	000001
	例2：JANコード型	491234567894	00000001
	・JANコード型の拡張	491234567894USA	000001
	例3：機器指定型	TC1234-0123	000001
指定者		お客様	システム生成

５．　検証システム

暗号化ＱＲシンボルの検証システムには、主に事業者向けを想定したスキャナを用いたシステムと主に消費者向けを想定してスマホを用いたシステムがある。

５．１　専用スキャナによる検証システム

専用スキャナを用いた検証システムを第８図に示す。また、用いる専用スキャナを第７表に示す。

ＴＣ－２３００は、赤外線照明ＬＥＤを具備しており、通常印刷の暗号化ＱＲシンボルだけでなく、透明の暗号化ＱＲシンボルを読取る事が可能である。また、ＴＣ－２２００は、通常の照明ＬＥＤであり、通常の印刷の暗号化ＱＲシンボルのみに対応する。

これらの専用スキャナをパソコンにＵＳＢ接続し、読取り結果を表示させることによって検証を行う。暗号化ＱＲシンボルの読取りができ、そこに収容されたデータが表示されることで、偽作の可能性は排除される。しかし、複製や複写の可能性は存在するので、検証対象のシンボルを数個読取り、固定部が当該商品に対応しているか、また、シリアル番号が全て異なっているかを確認して、複製、複写の可能性を判断する。

第８図　専用スキャナによる検証システム

第７表　暗号化ＱＲシンボル専用スキャナ

項目			TC-2200	TC-2300
スキャナ画像				
照明LED			可視光	赤外光
読取り可能シンボル	QRコード	通常印刷	○	○
		透明印刷	×	○
	暗号化QRシンボル	通常印刷	○	○
		透明印刷	×	○

５．２　スマホを用いた検証システム

スマホを用いた検証システムを第９図に示す。この検出システムは、通常印刷された暗号化ＱＲシンボルに対して検証を行う。暗号化ＱＲシンボルを読取るスマホ上で運用されるソフトウェアを無償で提供するので、消費者自身が簡単に検証を行うことが可能になる。

また、現在スマホに取り付けて用いる赤外線照明アダプターを開発中である。この赤外線照明アダプターを用いれば、スマホを用いて透明な暗号化ＱＲシンボルにも対応可能となる。

第９図　スマホによる検証システム

６．　応用システム

暗号化 QR シンボルを用いた応用システムについて紹介する。

６．１　物品の認証

第１の用途は、物品の認証用途である。物品の認証を行う対象の具体例を対象分野毎に、第８表に示す。

第８表　物品の認証

対象	具体例
有価証券	商品券、チケット、乗車券、紙幣
医薬品	包装箱、PTP、錠剤、アンプルシール
特定機器向け	インク、試薬、部品、部材
一般商品	工芸品、工業製品、美術品、食品

①有価証券

有価証券は印刷物であり比較的偽造、特に複写による偽造が多いと考えられる。そこで、透明化が有用である。また、紙幣を代表例として、既にシリアル番号が券面に印刷されているので、暗号化ＱＲシンボルに組込むシリアル番号と一致させることで、より正規性の確認が容易となる。第１０図に有価証券の例を示す。

第１０図　有価証券の例

②医薬品

医薬品の偽造抑止では、包装箱またはバイアルシールに暗号化ＱＲシンボルを付すことが中心となる。但し、ＰＴＰまたは錠剤単位での販売に対応するために、ＰＴＰまたは錠剤そのものに印刷することも可能である。

③特定機器向け

特定機器向けでは、特定機器で用いられる消耗品の偽造防止が目的である。多くの場合、正規品からの複製、複写がなされるので、透明印刷が望ましい。また、データ構成の固定部に特定機器の機器番号を記入することで、他の機器向けの商品の偽造を認証可能とする。当該機器向けの商品が偽造された場合には、シリアル番号の使用履

歴で認証する。

④一般商品

食品及び化粧品を除く一般商品では、暗号化ＱＲシンボルをシール形態で印刷し、当該シールを商品に貼付する。一方、食品や化粧品では、医薬品と同じく包装に印刷する。偽造抑止の観点からは離れるが、包装の美観が求められる場合には、暗号化ＱＲシンボルが透明印刷される。

６．２　書類等の認証

第２の用途は、書面の認証である。想定される書面の例を第９表に示す。書面の認証と物品の認証の違いは、対象の数量にある。物品では、大量の同一の物品が対象となる。一方書面では、対象が単一であるが、記載事項の異なる同一書式の書類が対象となる。そこで、シリアル番号による区別は不要となるが、内容毎に割振られた番号を対応させることで、検証が容易となる。

第９表　書面の認証

対象	具体例
人の認証	社員証、入門証、会員証、 資格者証、住民票、パスポート
口座の認証	クレジットカード、銀行カード
内容の認証	契約書、領収書、証明書

①人の認証

人の認証機能を有する書類等は、多く存在し、偽造に晒されている。一番多く用いられているのは、公的書類では運転免許証であろう。民間の書類では、社員証、学生証であろう。この他にも第９表に示すように多くの書類等がある。これらには、上記のように書類等に番号が付されているので、暗号化 QR シンボルのシリアル番号部をそれに一致させる。第１１図に社員証の例を示す。

第１１図　社員証の例

第１２図　クレジットカードの例

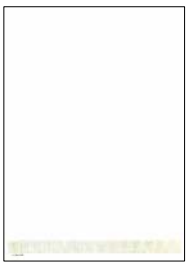
②口座の認証

クレジットカードや銀行カードでは、従前は磁気ストライプのみにデータが保持されていたが、セキュリティ向上のために、接触式 IC カードが採用されてきている。また、非接触式 IC カードも順次採用される方向にある。しかし、これらの IC カードは半導体を用いた電子機器であり、高価である。それに対して、暗号化 QR シンボルを透明印刷すれば、同様のセキュリティ性を維持しながら、より安価にシステム構築が可能となる。この場合には、シリアル番号に相当する口座番号及び使用者名、有効期限に対して、発行主体の金融機関の電子署名を付すのが適切である。第１２図にクレジットカードの例を示す。

③内容の認証

内容の認証は、契約書や領収書などの内容の認証であり、偽造、複製、複写を抑止し、原本であることを保証する。

具体的には、シリアル番号付き暗号化 QR シンボルが透明印刷された用紙を予め準備しておき、その用紙に手書きまたはプリンターで印刷する。この場合には、シリアル番号は透明 QR シンボルの下部などに追番印刷し、原本認証を容易にするとともに、用紙の原本管理を行う。第１３図に透明暗号化 QR シンボル付き用紙を示す。



第１３図　透明暗号化 QR シンボル付き用紙

７．終わりに

本稿では、シリアル番号付き暗号化 QR シンボルと開発した読取り機器、及びそれらを用いた偽造抑止の応用システムを紹介した。また、シリアル番号付き QR シンボルを透明化して、より偽造抑止効果を向上させる手法についても紹介した。

今後も、高付加価値の光学的情報媒体やその対応機器及びそれらの応用システムの開発に取り組んでいく所存である。

参考資料

１）JIS　X 0510:2018　(ISO/IEC 18004:2015)
２）月刊自動認識２０２０年３月号　秘匿領域と電子署名を有する菱形サブセルＱＲシンボル
３）月刊自動認識２０２０年９月号　透明な QR シンボルとそれに対応したスマートフォンによる認証と美観保持

参考動画

１．https://www.youtube.com/watch?v=C4O_m1SBNVM&t=5s　スマホによる透明ＱＲシンボルの読取り
２．https://www.youtube.com/watch?v=qwlkY0tWE5I　スキャナによる透明ＱＲシンボルの読取り

株式会社　テララコード研究所
お問合せ：mail@tcodes.jp　0562-74-5378